

NUMBER:	SP 961
EFFECTIVE:	08/01/2006
REVISION:	
PAGES:	2

Statement of.....

## Policy and Responsibility

---

SUBJECT: COMPUTER PASSWORD POLICY

---

### Computer Password Policy

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Murray City School District's (MSD) entire network. As such, all MSD computer users (including contractors and vendors with access to MSD systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

#### I. Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

#### II. Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any MSD facility, has access to the MSD network, or stores any non-public MSD information.

#### III. General

- A. All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a quarterly basis.
- B. All production system-level passwords must be part of the MSD's Technology Office administered global password management database.
- C. All user-level passwords with the exception of FIS users (e.g., email, web, desktop computer, etc.) must be changed at least once a year, at the beginning of the school year. The recommended change interval is every four months.
- D. FIS Users must be changed on at least a quarterly basis.
- E. User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user where practical.
- F. Passwords must not be inserted into email messages or other forms of electronic communication.

- G. Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
- H. All user-level and system-level passwords must conform to the guidelines described below.

#### **IV. Enforcement**

Any computer user found to have violated this policy may be subject to disciplinary action.

#### **V. Definitions**

Application Administration Account - Any account that is for the administration of an application (e.g., Oracle database administrator, ISSU administrator).

"sudo" - a program that allows a normal user access to administrative software.

SNMP - a type of management software used on the network by the Technology Office.